U.S. Patent No. 5,689,638, issued to *Sadovsky,* et al. ("*Sadovsky*"), in further view of "Reflexive Access Lists," published 5/5/1999, by Welcher, Peter J. ("*Welcher*"). The Office Action fails to present a prima facie case of unpatentability of Claims 1–9 and 13–19, 22–23, and 25–27 under 35 U.S.C. §103(a) because *Welcher* does not qualify as a prior art reference for this application under 102(a)/103(a). As supported by the Declarations by Inventors under 37 C.F.R. §1.131 included herewith, Applicants are entitled to a date of invention that is earlier than the effective date of *Welcher* as a reference. Accordingly, *Welcher* must be removed as a reference and the rejection should be withdrawn.

Even if *Welcher* is not removed as a reference, Claims 1–9 and 13–19, 22–23, and 25–27 are patentable over *Baize*, in view of *Sadovsky*, in view of *Welcher*, for the substantive reasons set forth below.

i. Welcher *not citable as prior art against application*

Effective date of *Welcher* as a reference

Welcher is a non-patent literature reference that was published on May 5, 1999. Applicants' application claims priority to U.S. Patent Application No. 09/347,433, filed July 2, 1999. Thus, the earliest effective filing date of *Welcher* as a reference is May 5, 1999, under 35 U.S.C. § 102(a). *Welcher* is not citable as a statutory bar under 35 U.S.C. § 102(b) or any other subsection of § 102. The Office Action cites *Welcher* under 35 U.S.C. §§ 102(a) and 103(a).

Applicants are entitled to a date of invention earlier than May 5, 1999

When any claim of an application or a patent under reexamination is rejected, the inventor of the subject matter of the rejected claim may submit an appropriate oath or declaration to establish invention of the subject matter of the rejected claim prior to the effective date of the reference or activity on which the rejection is based. 37 C.F.R. § 1.131. Upon proof of an earlier

date of invention by Applicants, the Office is required to withdraw the rejections that are made based on the reference. MPEP § 715. Applicants can establish prior invention of the claimed subject matter upon proof of (actual) reduction to practice the claimed invention prior to the effective date of the reference. MPEP § 715.07(II)(a). Furthermore, in contrast to interference practice, in which averments require corroboration, averments made in a 37 C.F.R. § 1.131 declaration do not require corroboration; an applicant may stand on his or her own declaration if he or she so elects. MPEP § 715.07(III).

Applicants are entitled to a date of invention earlier than May 5, 1999, because Applicants actually reduced to practice the claimed invention long prior to May 5, 1999. See Declaration of Tzong-Fen Fuh, Diheng Qu, and Serene Fan, May 21, 2008 ("Decl. Inventors"), submitted concurrently herewith.

Applicants conceived of and actually reduced to practice the invention prior to May 5, 1999

Applicants conceived of and actually reduced to practice the invention long prior to May 5, 1999. (Decl. Inventors, ¶3.) Applicants' conception and actual reduction to practice is established in the Declaration, and in the Exhibits to the Declaration, which comprise: "Authentication Proxy: Software Unit Functional Specification," a technical paper ("ENG-26866" hereinafter); "IOS Firewall Feature Set – Phase II Feature Test Plan," a technical paper ("ENG-30343" hereinafter); "Local Authentication of a Client of a Network Device," a patent disclosure record ("CPOL-37381" hereinafter). Taken together, ENG-26866 and CPOL-37381 constitute a complete disclosure of the claimed invention. (Decl. Inventors, ¶4.)

The Applicants' Declarations establish that testing according to the test plan as described in ENG-30343 was conducted and concluded long prior to May 5, 1999. (Decl. Inventors, ¶5) Applicants aver that the results of the tests sufficiently demonstrated that the invention worked

for its intended purpose long prior to May 5, 1999, and thereby establishing actual reduction to practice of the claimed invention before May 5, 1999. (Decl. Inventors, ¶5)

Although the dates of Exhibits to the Declaration have been blocked out, Applicants aver that the true dates of the conception of and actual reduction to practice of the claimed invention are long prior to May 5, 1999. Such an averment, supported by competent evidence here, fulfills all requirements of the case law, rules, and MPEP relating to proof of prior invention. Disclosure of the actual conception date is not required, because such a disclosure could seriously prejudice Applicants in any later interference proceeding. See MPEP § 715.07(II).

ENG-26866 and CPOL-37381 disclose all features of the present claims. The following table shows which parts of the documents disclosure the features of the claims. For purposes of this submission, Claims 1–9 and 13–19 are considered representative; all other claims have similar features. Further, the table below addresses only Claims 1, 15, and 22 because the Office Action only cites *Welcher* for Claims 1, 15, and 22.

Claim Feature	**Citation to Documents**
1. A system for controlling access of a client to a network resource, the system comprising: a network resource that is communicatively coupled to a network; a network firewall routing device that is communicatively coupled to the network and that is logically interposed between the client and the network resource, wherein the network firewall routing device comprises: a firewall that protects the network resource by means for selectively blocking messages initiated by client and directed to the network resource,	ENG–26866, Section 1.0, ¶ 1. CPOL–37381, Background. ENG–30343, Section 3.1, ¶ 1.

Claim Feature	Citation to Documents
wherein the firewall comprises: an external interface and an internal interface; and an Output Access Control List at the internal interface and an Input Access Control List at the external interface;	ENG–26866, Section 2.0, ¶¶ 2 & 3. CPOL–37381, Summary ¶¶ 1 & 2. ENG–30343, Section 3.1, ¶ 1.
an authentication server that is communicatively coupled to the network and to the network firewall routing device and comprising user profile information;	ENG–26866, Section 2.0, ¶¶ 2 & 3. CPOL–37381, Summary ¶ 1. ENG–30343, Section 3.1, ¶ 2.
means for creating and storing client authorization information at the network firewall routing device, based in part on the user profile information, wherein the client authorization information comprises information indicating whether the client is authorized to communicate with the network resource and information indicating what access privileges the client has with respect to the network resource;	ENG–26866, Section 2.0, ¶ 3. CPOL–37381, Summary ¶ 2. ENG–30343, Section 3.1, ¶ 3.
means for receiving a request from the client to communicate with the network resource;	ENG–26866, Section 2.0, ¶ 2. CPOL–37381, Summary ¶ 1. ENG–30343, Section 3.1, ¶ 2.
means for determining whether the client is authorized to communicate with the network resource based on the authorization information; and	ENG–26866, Section 2.0, ¶ 2. CPOL–37381, Summary ¶ 1. ENG–30343, Section 3.1, ¶¶ 2 & 3.

Claim Feature	Citation to Documents
means for reconfiguring the network firewall routing device to permit the client to communicate with the network resource only when the client is authorized to communicate with the network resource based on the authorization information, wherein the means for reconfiguring the network firewall routing device further comprises: means for determining a current IP address of the client; means for creating a new user profile information, based on the user profile information, that includes the current IP address; and means for adding the new user profile information as temporary entries to the Input Access Control List at the external interface and to the Output Access Control List at the internal interface.	ENG–26866, Section 2.0, ¶ 5. CPOL–37381, Summary ¶¶ 2 & 4. ENG–30343, Section 3.1, ¶ 5.
15. A system for controlling access to a network resource, the system comprising: a network resource that is communicatively coupled to a network; a client capable of sending a request to communicate with the network resource; a network firewall routing device that is logically interposed between the client and the network resource and is capable of permitting the client to communicate with the network resource, wherein the network firewall routing device comprises: a firewall that protects the network resource by selectively blocking messages initiated by client and directed to the network resource,	ENG–26866, Section 1.0, ¶ 1. CPOL–37381, Background. ENG–30343, Section 3.1, ¶ 1.
wherein the firewall comprises: an external interface and an internal interface; and an Output Access Control List at the internal interface and an Input Access Control List at the external interface;	ENG–26866, Section 2.0, ¶¶ 2 & 3. CPOL–37381, Summary ¶¶ 1 & 2. ENG–30343, Section 3.1, ¶ 1.

Claim Feature	Citation to Documents
an authentication server that is communicatively coupled to the network and to the network firewall routing device and comprising user profile information;	ENG–26866, Section 2.0, ¶¶ 2 & 3. CPOL–37381, Summary ¶ 1. ENG–30343, Section 3.1, ¶ 2.
means for creating and storing client authorization information at the network firewall routing device, wherein the client authorization information comprises information indicating whether the client is authorized to communicate with the network resource and information indicating what access privileges the client has with respect to the network resource;	ENG–26866, Section 2.0, ¶ 3. CPOL–37381, Summary ¶ 2. ENG–30343, Section 3.1, ¶ 3.
means for determining, at the network firewall routing device, whether the client is authorized to communicate with the network resource based on the authorization information; and	ENG–26866, Section 2.0, ¶¶ 2 & 3. CPOL–37381, Summary ¶¶ 1 & 3. ENG–30343, Section 3.1, ¶ 4.
means for reconfiguring the network firewall routing device to permit the client to communicate with the network resource only when the client is authorized to communicate with the network resource based on the authorization information, wherein the means for reconfiguring the network firewall routing device further comprises: means for determining a current IP address of the client; means for creating a new user profile information, based on the user profile information, that includes the current IP address; and means for adding the new user profile information as temporary entries to the Input Access Control List at the external interface and to the Output Access Control List at the internal interface.	ENG–26866, Section 2.0, ¶ 5. CPOL–37381, Summary ¶¶ 2 & 4. ENG–30343, Section 3.1, ¶ 5.

Claim Feature	Citation to Documents
22. A system for authentication comprising: a network resource connected to a network; a client capable of sending a request to communicate with the network resource; a network firewall routing device that is logically interposed between the client and the network resource and that is reconfigured to permit the client to communicate with the network resource only when the client is authorized to communicate with the network resource based on client authorization information stored in the network firewall routing device,	ENG–26866, Section 1.0, ¶ 1. CPOL–37381, Background. ENG–30343, Section 3.1, ¶ 1.
wherein the network firewall routing device comprises: a firewall that protects the network resource by means for selectively blocking messages initiated by client and directed to the network resource, wherein the firewall comprises: an external interface and an internal interface; an Output Access Control List at the internal interface and an Input Access Control List at the external interface;	ENG–26866, Section 2.0, ¶¶ 2 & 3. CPOL–37381, Summary ¶¶ 1 & 2. ENG–30343, Section 3.1, ¶ 1.
wherein the network firewall routing device, when reconfigured, is reconfigured by the steps of: determining a current IP address of the client; creating a new user profile information, based on the user profile information, that includes the current IP address; and adding the new user profile information as temporary entries to the Input Access Control List at the external interface and to the Output Access Control List at the internal interface; and	ENG–26866, Section 2.0, ¶ 5. CPOL–37381, Summary ¶¶ 2 & 4. ENG–30343, Section 3.1, ¶ 5.
wherein the client authorization information comprises information indicating whether the client is authorized to communicate with the network resource and information indicating what access privileges the client has with respect to the network resource;	ENG–26866, Section 2.0, ¶ 3. CPOL–37381, Summary ¶ 2. ENG–30343, Section 3.1, ¶ 3.

Claim Feature	Citation to Documents
a database server that stores a plurality of user profiles, each user profile uniquely associated with one of a plurality of users that can use the client to send requests to communicate with the network resource;	ENG–26866, Section 2.0, ¶ 3. CPOL–37381, Summary ¶ 2. ENG–30343, Section 3.1, ¶ 3.
an authentication server that is logically interposed between the network firewall routing device and the database server, and that is capable of communicating with the database server and retrieving from the database server a user profile.	ENG–26866, Section 2.0, ¶¶ 2 & 3. CPOL–37381, Summary ¶ 1. ENG–30343, Section 3.1, ¶ 2.

The Declaration submitted herewith and the remarks herein establish that Applicants are entitled to a date of invention earlier than the effective date of *Welcher* as a reference. Therefore, *Welcher* is not citable as prior art against the application. Applicants respectfully request that all rejections based on *Welcher* be withdrawn.

ii. *Claims 1–9 and 13–19, 22–23, and 25–27 patentable over BAIZE in view of SADOVSKY in view of WELCHER*

Claims 1–9 and 13–19, 22–23, and 25–27 are rejected under 35 U.S.C. § 103(a) as allegedly obvious over *Baize*, in view of *Sadovsky,* in view of *Welcher*. Notwithstanding Applicants' contentions that *Welcher* is not citable as prior art against the application, the rejections based on the cited art are respectfully traversed in the following discussion.

Independent Claim 1 recites:

> ....
>
> **means for reconfiguring the network firewall routing device to permit the client to communicate with the network resource only when the client is authorized to communicate with the network resource based on the authorization information,** wherein the means for

> reconfiguring the network firewall routing device further comprises:
>
> means for determining a current IP address of the client;
>
> means for creating a new user profile information, based on the user profile information, that includes the current IP address; and
>
> means for adding the new user profile information as temporary entries to the Input Access Control List at the external interface and to the Output Access Control List at the internal interface.

(Emphases added.) According to one embodiment of the invention, the network firewall device is reconfigured by means for adding new user profile information to access control lists that at the external interface and the internal interface of the firewall **only when the client is authorized to communicate with the network resource based on the authorization information**. As discussed in the previous Reply to Office Action submitted by Applicants on July 10, 2007, one possible benefit of reconfiguring a part of the network firewall routing device is that the configuration is maintained indefinitely until certain conditions are met, for example, a timeout or a specific modification by the system administrator. This allows the logical passageway to remain open even if the user and client encounters an inadvertent or transient disconnection. (Paragraph [0091].) Using this method, the session is not reset by the disconnection, and the firewall does not need to access the authentication server when the user or client re-establishes the connection.

No combination of *Baize*, in view of *Sadovsky*, in further view of *Welcher*, discloses each and every express element of Claim 1. Neither *Baize*, *Sadovsky*, nor *Welcher* teach or disclose means for reconfiguring a firewall **only when the client is authorized to communicate with the network resource based on the authorization information**. Neither *Baize* nor *Sadovsky* teaches or discloses means for adding new user information that includes **current IP address as**

temporary entries. Instead, *Baize* teaches that an operational user profile is fetched from the security server, and "any subsequent request to another server or resource may be allowed or denied according to said operational profile." (*Baize*, Col. 7, lines 3–5.) *Baize* teaches that a subsequent request is allowed or denied by "[applying] the application rules (module 50) according to the operational profile." (*Baize*, Col. 7, lines 12–14). However, "applying the application rules," as taught by *Baize*, does not teach or disclose the particular means for reconfiguring the firewall as recited in Claim 1.

The Office Action also relies on *Sadovsky* to teach and disclose means for reconfiguring a network firewall routing device. However, *Sadovsky* does not teach any means for reconfiguring a firewall comprising means of adding temporary entries to access control lists. *Sadovsky* merely teaches maintaining a cache of usernames and passwords at a central server. It does not teach any user profile information, or any client authentication information that indicates any access privileges the client has with respect to the resource, as recited in Claim 1. It does not teach creating any new user information data that includes any current IP addresses. Therefore, *Sadovsky* does not "fill the gaps" that *Baize* leaves with respect to Claim 1.

The Office Action relies on *Welcher* to teach and disclose means for "means for reconfiguring the network firewall routing device to permit the client to communicate with the network resource only when the client is authorized to communicate with the network resource **based on the authorization information,**" as recited in Claim 1. In contrast to Claim 1, nowhere in *Welcher* is it described to dynamically add or remove entries from the temporary access lists based on any authorization information. Instead, *Welcher* describes temporary access list entries "whenever new outbound traffic is seen." (*Welcher*, Subsection "What are Reflexive

Access Lists," Paragraph 4.) Accordingly, *Welcher* fails to teach the full detail of the feature as recited in Claim 1, and thus, fails to fill the gaps left by *Baize* in view of *Sadovsky*.

Because no combination of *Baize*, in view of *Sadovsky*, in view of *Welcher*, teach the complete claimed subject of Claim 1, it is respectfully submitted that Claim 1 is patentable over the cited art.

Independent Claim 15 and 22 include features similar to Claim 1. It is therefore respectfully submitted that Claims 15 and 22 are patentable over *Baize*, in view of *Sadovsky*, in view of *Welcher*, for at least the reasons given above with respect to Claims 15 and 22.

Claims 2–9, 13–14, 16–19, 23, and 25–27 are dependent claims, each of which depends (directly or indirectly) on Claims 1, 15, and 22. In addition, each of Claims 2–9, 13–14, 16–19, 23, and 25–27 introduces one or more additional features that independently render it patentable. Due to the fundamental differences already identified, to expedite the positive resolution of this case, a separate discussion of the features of Claims 2–9, 13–14, 16–19, 23, and 25–27 is not included at this time. The Applicant reserves the right to further point out the differences between the cited art and the novel features recited in the dependent claims.

B. CLAIM 12 —*BAIZE in view of SADOVSKY in view of WELCHER, in further view of COSS*

Claim 12 were rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Baize*, in view of *Sadovsky*, in view of *Welcher*, in further view of U.S. Patent No. 6,170,012 issued to *Coss* et al. The rejections are respectfully traversed.

Claim 12 is a dependent claim, which depends (directly or indirectly) on Claim 1. The Office action relies on *Coss* for teaching the limitations within those dependent claims. However, *Coss* does not "fill the gaps" that *Baize* and *Sadovsky* leave with respect to

independent Claim 1. Any combination of *Baize*, *Sadovsky*, *Welcher* and *Coss* fails to provide the complete claimed subject matter of Claim 1. Due to the fundamental differences already identified, to expedite the positive resolution of this case, a separate discussion of the features of Claim 12 is not included at this time. In addition, Claim 12 introduces one or more additional features that independently render it patentable. The Applicant reserves the right to further point out the differences between the cited art and the novel features recited in the dependent claims.

C. CLAIMS 10–11, 20–21, 24, and 28–30 —*BAIZE in view of SADOVSKY in view of WELCHER, in further view of KLASSEN*

Claim 12 were rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Baize*, in view of *Sadovsky*, in view of *Welcher*, in further view of U.S. Patent No. 6,170,012 issued to *Klassen* et al. The rejections are respectfully traversed.

Claims 10–11, 20–21, 24, and 28–30 are dependent claims, each of which depends (directly or indirectly) on Claims 1, 15, or 22. The Office action relies on *Klassen* for teaching the limitations within those dependent claims. However, *Klassen* does not "fill the gaps" that *Baize*, *Sadovsky* and *Welcher* leave with respect to independent Claims 1, 15, or 22. Any combination of *Baize*, *Sadovsky*, *Welcher*, and *Klassen* fails to provide the complete claimed subject matter of Claims 1, 15, or 22. Due to the fundamental differences already identified, to expedite the positive resolution of this case, a separate discussion of the features of Claims 10–11, 20–21, 24, and 28–30 is not included at this time. In addition, each of Claims 10–11, 20–21, 24, and 28–30 introduces one or more additional features that independently render it patentable. The Applicant reserves the right to further point out the differences between the cited art and the novel features recited in the dependent claims.